2019

Procure-to-Pay Software in the Digital Age: An Exploration and Analysis of Efficiency Gains and Cybersecurity Risks in Modern Procurement Systems

Drew Lane
University of Kentucky, drew.lane@uky.edu

Procure-to-Pay Software in the Digital Age

An Exploration and Analysis of Efficiency Gains and Cybersecurity Risks in Modern Procurement Systems

Lane, Drew
THE MARTIN SCHOOL OF PUBLIC POLICY AND ADMINISTRATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Procure-to-Pay (P2P) softwares are an integral part of the payment and procurement processing functions at large-scale governmental institutions. These softwares house all of the financial functions related to procurement, accounts payable, and often human resources, helping to facilitate and automate the process from initiation of a payment or purchase, to the actual disbursal of funds. Often, these softwares contain budgeting and financial reporting tools as part of the offering. As such an integral part of the financial process, these softwares obviously come at an immense cost from a set of reputable vendors. In the case of government, these vendors mainly consist of Oracle, SAP and Jagger.

This paper will explore the evolution of P2P software from its birth as an IBM solution to strategic sourcing issues, to the current cloud-based, end-to-end procurement and payment software suites that millions of private enterprises and an increasing amount of governments now enjoy. It will also explore the risks associated with "the cloud", an industry term for constantly connected online services where data and software are provided off-premises from the purchasing institution. These services often house all of the financial data related to the institution, safeguard it and provide consistent updates throughout the licensing term. However, as an expense, these softwares can be difficult to market to taxpayers, who ultimately pay for software upgrades.

This paper concludes, after analysis of literature, financial data and interviews with key stakeholders in the decision-making process, that these softwares provide significant efficiency gains, but can pose a new form of misunderstood cybersecurity risks. This combination of the "newness" of cloud computing and immense costs stretched over years can make it difficult for

governments—especially smaller governments—to convince taxpayers that these system upgrades are worthwhile.

INTRODUCTION TO THE ISSUE

Procure to Pay Software's Beginnings

P2P software has existed in principle since the creation of the computer. The idea of automating payment systems and reducing an organization's load of transaction processing has been forefront ever since computers have been an accessible expense for companies and governments. However, the beginning of P2P as a service offered to organizations can be traced to IBM in the year 2000, when it patented an internal requisition management system that automatically reordered components used in the manufacturing of the company's computers. It was not until the mid 2000s when companies like Oracle, SAP and Jagger began pitching their own, now robust P2P management systems to governments. Throughout the 80s, these companies marketed accounting software to assist companies in the streamlining of accounting processes. However, it was not until 1995, when SAP released SAP R/3, that Enterprise Resource Management (ERM) programs took the forefront of sales portfolios, and it was not until 2006 that these products were actively connected with server networks and the internet, allowing large-scale access within an organization.

"The Cloud" and P2P's Revolution

"The Cloud" is a term for an always connected software or service that stores, emulates, backs-up and processes data. Many common examples of cloud-based systems exist, but most private users are more familiar with document-storage services like Google Drive, Microsoft

OneDrive, and Apple's iCloud, which do not emulate software. Microsoft recently pushed most of its Office software online with Office 365, which provides continual software updates and online, emulated versions of its programs like Word, PowerPoint and Excel for a monthly subscription fee. The model became known as "software-as-a-service." These services created the P2P revolution in cloud-based computing, as consumers began to understand and adopt the model.

Cloud-based P2P began in 2012, with the introduction of Oracle's Oracle Cloud software, which ran natively on Oracle's servers, and was projected to end-users' computers. SAP acquired Ariba, a cloud-based P2P system and Concur to compete with Oracle in the market, eventually integrating them into the SAP 4/HANA architecture, which provides ERM for subscribers (SAP, 2019). These softwares took the "software-as-a-service" model and applied it to large-scale private companies that could afford them, claiming reduced IT costs over time and significant efficiency gains at subscribing organizations. Companies no longer needed to purchase powerful computers that were capable of running suites of Oracle or SAP software because the software ran natively on the provider's servers. Providers also assumed the risk and responsibility of managing cybersecurity and consistent updates, reducing the burden on end users.

Willingness of Taxpayers to Pay for System Upgrades

Despite these benefits, providers couldn't seem to convince governments to subscribe to expensive software updates, as many had legacy systems that were purchased to process payments in the 1990s or 2000s. Outside of large-scale public and private research universities, which procure a wide-range of services and goods for research and teaching courses, city and

state governments were largely hesitant to upgrade from expensive software suites that had been purchased in the past. Many, like the federal government, designed their own systems or heavily modified stock versions of SAP and Oracle to fit their respective institutions.

Software upgrades in the private sector are not typically an issue. Large companies like Apple, Microsoft and Google all adopted eProcurement systems (like Ariba) early in the process, as they are not beholden to taxpayers or key stakeholders outside of shareholders. Financial reports for these private companies are not as publicly disseminated as a government's CAFR.

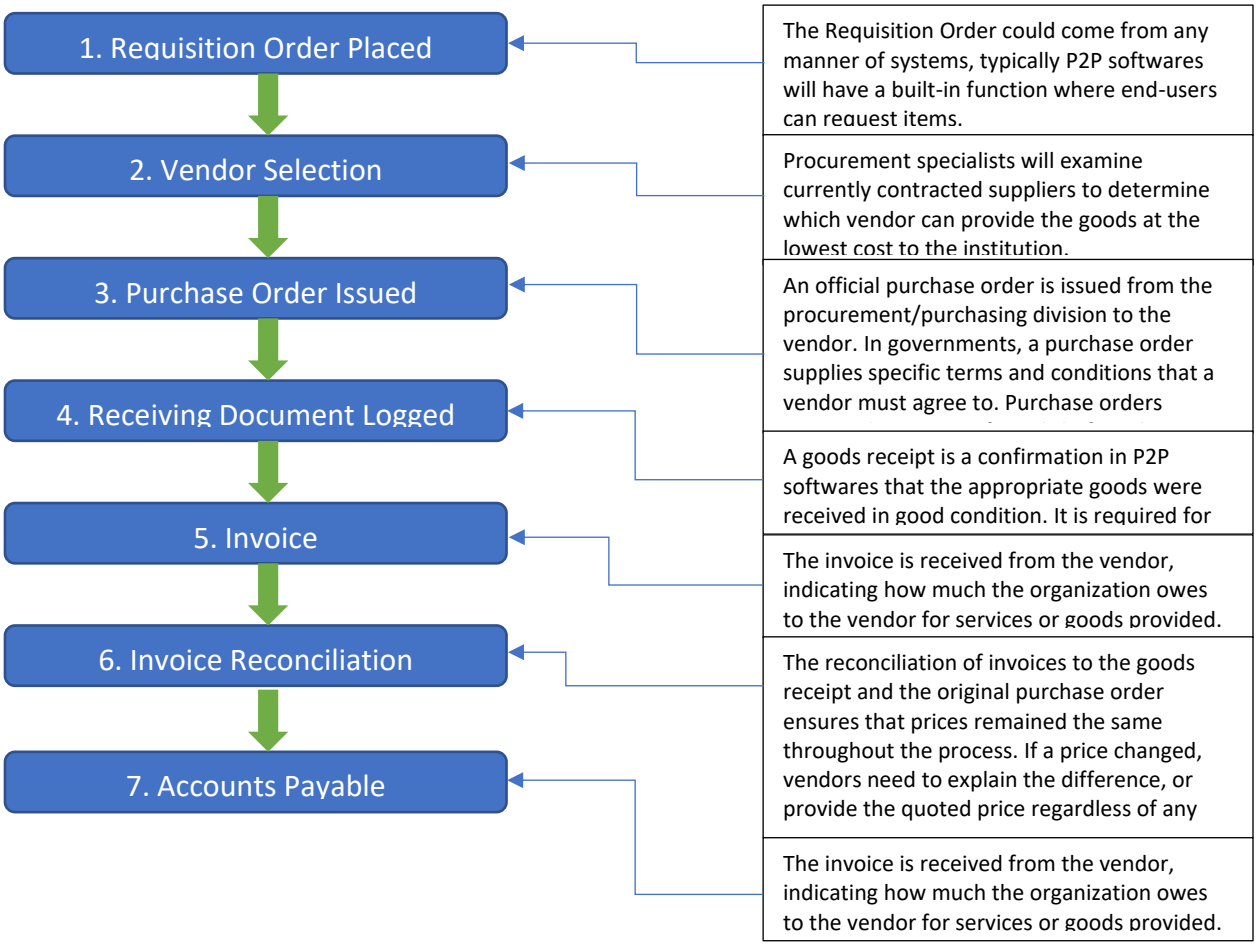
In government, these expenses are very public and subject to scrutiny through public discourse, the media and lawmakers themselves. In 2018, the City of Lexington, KY upgraded its Oracle PeopleSoft software for HR functions and spent $5.1 million on that upgrade alone (LFUCG, 2018). Taxpayers should question the cost benefits of these softwares, and governments must extensively communicate the benefits to the taxpayers.

LITERATURE REVIEW

The Procure to Pay Process

The P2P process itself consists of several stages and workflows for each function (purchasing, accounts payable, etc). This paper focuses primarily on procurement and will outline and define the procurement process from that framework. P2P is not the actual process of procurement, rather, it is a term the industry has created to discuss the automation of the procurement process itself, from the initiation of the procurement action to cash disbursement to vendors. Figure 1 demonstrates the P2P process, according to Rob Biedron at *Purchase Control* (2018):

FIGURE 1: The P2P Process



This process varies widely from organization to organization and can take many forms. This is in no way the sole P2P process, but it reflects the vast majority of processes across government entities.

The Proliferation of P2P Software and its Evolution

P2P softwares have played a role in the private sector since 2000, when IBM patented a software for automating and digitizing the replenishment process in manufacturing their computers (Farias & Romo, 2000). From there, companies like SAP, Oracle and others have

created and marketed their softwares to organizations, first primarily to the private sector, and more recently to governments. Currently, SAP, the industry leader in procurement and Enterprise Resource Management (ERM) softwares, and their P2P offering, Ariba, is used by over 3.6 million businesses (SAP, 2019). Ariba, and many of the other large-scale platforms that unify procure-to-pay processes can be scaled down to smaller governments and implemented as a full system or as a single piece. For example, one company could simply use SAP Concur for travel reimbursements, while another uses Concur for travel, Ariba for purchasing, and HANA for ERM and analytics together as one unified system at an increased cost.

While many organizations have onboarded P2P systems over the years, several quasi-governmental organizations historically lag behind the private sector, particularly healthcare (HFM, 2018). Healthcare, like many governmental organizations, works under intensive scrutiny and regulations like HIPAA, making automation difficult—if not impossible in some cases. However, even eProcurement and ePayments to vendors are beginning to proliferate in these segments, representing a shift to paperless and electronic workflows in some of the most bureaucratic areas of the government.

However, the largest shift has been in the recent change to cloud-based procurement systems, and with it, the entire model for P2P software purchases has changed. Previously, organizations seeking to implement P2P software to increase efficiency and internal control strengths were required to purchase a software package from the software developer, an organization like SAP or Oracle. In some cases, organizations like the federal government built their own systems. These were highly customizable, but required a team of software engineers to maintain and develop functionality as processes changed. With the introduction of cloud-

based procurement systems, software is always up-to-date, and data is stored in “the cloud”, a term for internet servers which conduct the majority of computing and data storage housed outside of the organization. Notably, the initial sticker-shock associated with a large-scale implementation of SAP has diminished—cloud-based systems require a monthly or annual subscription fee, rather than a complete payment up-front, easing budgetary restrictions on organizations (Center for Digital Government, 2018). This is often called “software-as-a-service” (Miller, 2017). We are all familiar with the software-as-a-service model, from Microsoft Office 365 for productivity at home, to Netflix for streaming entertainment, each of these charge a monthly fee to access the software and services required, and it is always up to date. In the 1990s to the mid 2000s, software was purchased once, and if an end-user wished to upgrade, they needed to purchase another full version of the software. Microsoft Office was an excellent example of this, as it was released every year. Members with Office 2016 did not get Office 2017 as a free upgrade, rather they needed to purchase the software again. P2P was like this in its early days too. Now, much like Office 365’s $9.99 per month subscription fee, cloud based P2P is becoming a software-as-a-service rather than a one-time purchase.

The goal of the shift to this new cloud-based platform is flexibility. Governments see the future of procurement and technology as flexible, and entities need to react to shifts in the environment as quickly as possible. Antiquated systems are less flexible because software needs to be developed at the end-user’s organization, typically through an Enterprise Application Team. It is costly and often creates unintuitive systems (Miller, 2018). The shift to the cloud means software is developed on the provider’s end and is implemented as a software update included in the subscription cost, making the software longer-lived and more capable of

responding to shifts in the environment. However, it is notable that the growth in adoption of these systems is partly driven by governments feeling left out if they do not adopt the technologies, even if current systems in place work as they are (Sanderson, Lonsdale, Mannion, et. al, 2015).

Developing and implementing a plan for more intuitive and flexible systems increases cost savings over time. Added flexibility in procurement processes and improved user experiences with newer softwares help organizations control spending by keeping end-users on-contract. Negotiated purchasing contracts reduce costs for the institution, and when they are ignored because e-commerce websites like Amazon are easier to navigate, spending will inevitably increase over time. Most cloud-based P2P systems provide a more familiar experience, much like shopping online on any website. This also helps improve internal controls and reduce the risk for fraud. By reducing the amount of off-contract purchases, the institution can keep more within the workflows in the P2P system, allowing for multiple levels of approvals over transactions that once were made by a single individual with a procurement card and no oversight.

Cybersecurity in the Digital Age

As the world turns more and more to online services as a method of processing transactions, and those softwares migrate online to the cloud and off of local servers, it raises a critical question: what about cybersecurity? Both of the largest software makers, SAP and Oracle, have entire sections of their online presence dedicated to cybersecurity and the trustworthiness of their software against attacks from malicious forces. Old softwares were housed locally within an organization, meaning the data was not necessarily stored online, and

no Internet connection was required to access the financial data organizations need to process transactions. The newer, cloud-based systems store all information online, typically with the provider itself. SAP (2019) argues that, "...contrary to popular belief, cloud security standards are surpassing traditional on-premise security standards. Key security concerns are the same in the cloud or on premise, and include the risk of external attack or malicious insider activity." Despite the improvements in cloud-based cybersecurity, governments are accountable to the public for keeping financial data safe, and it may be difficult to explain moving data from the government's own servers to servers of a private company and connecting that data to the Internet.

A critical case study of these risks is Baltimore, Maryland, which recently struggled with a cyber attack that crippled P2P and other key governmental functions like water billing, real estate sales and healthcare services. An NSA-developed cyberweapon—codenamed EternalBlue—wreaked havoc on the systems, destroying computers and downing the entire city's email service (Pelroth & Shane, 2019). Such cyberweapons can cause impacts at every level of government, and could potentially disrupt internet services, phone services, power grids, and other critical infrastructure. After observing the multitude of EternalBlue hacks, public administrators seeking to move critical systems to the internet and into technology should heavily consider cybersecurity as one of the largest risks to P2P software and any efficiency gains they may bring. While the Baltimore incident was one example, other examples, like North Korea's WannaCry hack, demonstrate that foreign countries could attack financial systems. Despite software developers like SAP's insistence that their servers are safe, centralizing governmental financial data with one—or even a few—companies online exposes

more than just one organization to a cyberattack. If SAP alone were the victim of such an attack, nearly 3.6 million governments, businesses and vendors would be exposed to a disruption of services and potential theft of financial data. With Baltimore's current system, data was housed within its own servers, limiting the scope to one city rather than systems across the nation.

The argument for flexibility in P2P software-as-a-service as it migrates to the cloud comes with this enhanced risk that data for thousands of government entities could be breached at once, limiting and disrupting service for millions of customers.

RESEARCH DESIGN

My research takes into account the primary focus of this paper: 1) *Can the proliferation of Procure-to-Pay (P2P) software improve efficiency and mitigate risks in the digital age as softwares shift online?* 2) *Can these upgrade costs be justified to taxpayers?*

As discussed in the literature review, I examined a variety of sources to holistically research the topic and determine the viability of these softwares in the public sector, particularly focusing on the rapid proliferation of the softwares, the variety of softwares offered (including those built independently), and the risks they may expose organizations to as data shifts online. In order to do so, I have consulted as many publications as possible on the subject. It must be addressed that there is not much academic research or extensive coverage of P2P systems at the government level, and marketing materials for major software providers had to be used to find the breadth and scope of these implementations.

The remainder of the research is conducted with interviews with key stakeholders in deciding the P2P software strategy at different levels of government, including The University

of Kentucky's Chief Procurement Officer Barry Swanson, the University of Kentucky's Executive Director of Auxiliary Services James Frazier, and cybersecurity expert Matt Perry.

Additionally, The University of Kentucky has been used as a case study for efficiency data and as an example for maintenance costs of antiquated systems that predated the online cloud network of the modern era. The University of Kentucky also is used as an example in transition from an antiquated system to a cloud-based, "software as a service" system and data is presented that compares current legacy SAP costs to expected new SAP maintenance costs.

The purpose of using the University of Kentucky is two-fold: one, the University is actively seeking, through an RFP, a new cloud-based eProcurement provider and the budgetary impacts and financial efficiency savings will be an example for other institutions exploring this change. While cloud-based systems are prevalent in the private sector, universities and governments face challenges in justifying large financial software purchases to constituents (or students) and tend to use software beyond its useful date. Two, the university has just completed the process of analyzing and justifying the costs of P2P software internally, and in the public sector through press releases.

In analyzing cybersecurity risks, I used the publicly available data from the 2018 Council of Economic Advisors report on the "Costs of Malicious Cyber Activity to the U.S. Economy" and several case studies, including the Baltimore cyberattack discussed in the literature review, to analyze the risks posed when moving data from a disconnected local server (called "on-prem") to the cloud. Other cases were examined to determine effective risk mitigation tactics for cloud-based systems, particularly processes in place in governments to prepare for loss-of-

service or disruption-of-service losses related to continuously connected softwares, including productivity suites.

ANALYSIS AND FINDINGS

This section will explore my analysis of available data and interviews surrounding cloud-based P2P software, its efficiencies and the risks that follow its implementation—particularly cybersecurity. This is the most important aspect financial managers should weigh when considering a costly software upgrade, as cyberattacks are costly and run the risk of completely incapacitating the financial functions of a government. In understanding this risk, I explore each side of P2P software, both on-premise and in the cloud, as well as the financial risks and considerations for public financial managers who make budgetary decisions for software maintenance and upgrades.

KEY FINDINGS:

- Cloud-based P2P software provides significant cost savings in efficiency gains and maintenance costs.
- Cybersecurity risks, when exploited by malicious actors, are costly and can cripple government.
- Government data, when properly protected, is safer in the cloud because of the built-in redundancies in the software.
- Public financial managers should implement cybersecurity plans and allocate resources to the protection of system integrity, as costs associated with a breach can cripple government.

Financial and Efficiency Benefits

The financial benefits of pushing risk to a third-party provider are numerous. Historically, as software has evolved over time, it has become capable of more and more functions, speeding up workflows and employee productivity. The new P2P programs integrate

many previously-separated functions into one cohesive workflow. For example: SAP Ariba recognizes each requisition requestor and assigns a default account and shipping information to each. Previously, in SAP's legacy system, a requestor had to make the request, while a business officer would enter financial transactions and assess funding availability for the purchase. In these new systems, an entire step has been removed, which frees staff to work on other important goals in their offices.

However, an overstaffed government that transitions to a newer P2P software may find that so many legacy processes are eliminated that the efficiency savings are realized further in workforce reduction. While this is never a positive for staff, reductions in the workforce processing transactions frees dollars to reallocate staff in other areas that desperately need it. This draws back to Miller's "flexibility" argument—the less bloated a government is with redundant processes and overstaffed IT and Business Offices, the quicker it can react to shifts in the environment.

Another key financial and efficiency saving is the role the provider takes in maintaining servers, IT, security and software development. In most legacy systems, once the software purchase is completed, the organization was responsible for staffing software developers, cybersecurity experts and server maintenance teams. At a large-scale institution, the yearly staffing costs for Enterprise Application IT can cost millions of dollars. By shifting these core IT responsibilities (particularly the duty to update and develop software) to an external party, the institution itself not only shifts risks, but also allows for workforce reallocation or reduction.

The immediate efficiency gains and financial savings are compelling, however, there are significant investments that must be made to realize these savings. Initial costs can be in the

tens of millions with recurring license fees. Because the entity no longer outright owns the software, it must continue to pay recurring licensing fees, which vary from provider to provider. Governments particularly should analyze the budget impact that these license fees will have and should work to fully understand the impacts in both healthy and unhealthy budget situations. High licensing fees that are recurring can put strain on a budget over time, particularly in times of economic stress. The one-time implementation fee of a legacy system was easily predictable and could be paid at a time of economic prosperity or a budget surplus. Failure to pay P2P licensing fees for cloud-based systems would disable functionality, and potentially disable the government's financial transaction processing.

End-User Experience

One of the largest benefits to new, cloud-based P2P softwares is the end-user experience. Legacy systems are often a mix of generic software (which was part of the original purchase) and custom additions, which can lead to an often disjointed and unintuitive end-user experience. The critical point Swanson made in our discussion was how important this aspect was to The University of Kentucky's decision to migrate to cloud-based systems. In SAP Ariba, when integrated with SAP 4/HANA and SAP Concur, the three systems provide a unified user interface that allows end users to shop in an environment similar to online retailers like Amazon, except all of the offered items are on-contract, and reduce the overall expenses of procurement at an institution.

With legacy systems it is difficult to reign-in spending. Outside vendors are often easier to navigate than preferred vendors or require special access to browse. The modernization of the end-user experience makes it easier for key stakeholders, business officers, and

procurement card holders to manage their account balances, make requisition requests and track workflows through internal approver stages. Institutions (and the providers themselves) argue that by improving the end-user experience, remaining on contract is easier, thus reducing overall spend. This quoted savings is estimated at over $13 million for The University of Kentucky's shift to cloud-based SAP Ariba. These savings can be reallocated to other projects at the University, like improving the student experience or increasing the amount of faculty available to students.

The On-Premise v. Cloud Debate

Drawing from conversations with Barry Swanson, James Frazier and Matt Perry, this section's analysis focuses primarily on interviews and some literature surrounding the ongoing debate on the security benefits of "on-premise" P2P softwares (commonly referred to as on-prem), and cloud-based softwares. This section of my research is the most heavily subjective, because the answer differs from organization to organization based on their needs. However, I have created three categories of government P2P systems to simplify my determinations. The first two categories represent large-scale, multi-billion-dollar organizations: Cloud Heavy Entities and Legacy Dependent Entities. The third category is representative of other governments of different sizes, called Small-Scale Entities.

FIGURE 2: List of Case Studied Entities and Classification

Entity Name	**Classification**	**Reasoning**
Lexington-Fayette Urban County Government	Legacy Dependent Mix	The LFUCG runs legacy accounting softwares integrated with cloud-based Oracle PeopleSoft.
The University of Kentucky	Legacy Dependent	UK runs all P2P functions with a version of SAP implemented in 2005
The City of Baltimore	Small-Scale	While Baltimore is a large city, it depends on a self-designed and maintained form of P2P systems, much like many small-scale entities.
Riviera Beach, Florida	Small Scale	
Lake City, Florida	Small Scale	

On-Premise

There are many benefits to on-prem software and data management, the primary being the organization owns, stores and protects its data on-premises, meaning the servers that house the data and emulate the software are maintained within an organization, or at an off-

site location owned by the entity. At the University of Kentucky, servers are housed throughout campus in various locations. The City of Baltimore houses a mix of systems on owned servers across the government. Both employ large IT and Enterprise Application specialists to maintain and manipulate the software to fit the institution's needs. At The University of Kentucky, this team consists of 52 members, housed within the ITS Enterprise Applications Department, at a cost of $4,444,631 in FY2019 (Robinson, 2019). This is one of the largest downsides of on-prem data management. While not all salaries in the group are dedicated solely to SAP maintenance, a quality Enterprise Applications Group will cost significant sums year-over-year in salary alone.

According to Matt Perry, on-prem data management is less likely to experience a cybersecurity event, however, when one occurs, it is more likely to get through any defenses the group has put in place. In Baltimore City, the EternalBlue cyberattack successfully infiltrated the firewall when an employee clicked a link in an email, granting access to the systems (Pelroth & Shane, 2019). Key in the debate is redundancies of the data and software—or making backups of the data and software so a new version can run while others may be compromised. In Baltimore's case, there were no redundancies in place, and the EternalBlue ransomware downed the city's email servers and key systems across the government.

On-prem, legacy systems with poor maintenance and outdated security protocols pose the greatest risks, as the City of Baltimore proves. Many organizations, including The University of Kentucky, engage in employee information campaigns to educate staff on the hallmark traits of a malicious email: strange domain names, spelling errors and unnatural phrasing—among many others. Older systems, and unsupported, unsecure operating systems like Windows 7 are still used in a large swath of the public. Windows 7, which has been unsupported for years

following the release of Microsoft's Windows 10, is still installed on 36.9 percent of Windows machines (Warren, 2019). Security patches no longer keep these outdated operating systems protected against threats. On-prem P2P software is similar, as the IT departments at respective organizations must alter and update the code to make these systems more secure against external threats.

In the month of June 2019, two cities in Florida, Riviera Beach and Lake City both paid $600,000 and $426,000 respectively in Bitcoin to hackers that disabled a number of systems from credit card processing to the city's email service. Smaller governments like Riviera Beach and Lake City are much more susceptible to attacks, but they are not the only victims. Before the two Florida attacks, there were 22 breaches of public systems across the US (Ahmed, 2019). Large cities like Baltimore or Atlanta (which has more advanced P2P software) have both seen cyberattacks that forced employees to perform services manually while waiting to restore service. Because on-prem data storage is more likely to be implemented at a smaller institution that may be resistant to modernization and low-staffed, these small-scale, legacy dependent organizations are at the most risk.

The Cloud

Cloud-based P2P softwares offer many benefits over on-prem software maintenance, particularly in the case of smaller organizations who may not have the ability to properly protect and secure their servers from threats. However, there are risks to storing governmental data in the cloud on centralized, third-party servers. The most important consideration is the cybersecurity reputation and track-record of the vendor. As with on-prem, this varies widely based on the provider. Providers like Oracle and SAP are some of the most secure software

services, and according to Matt Perry, likely experience thousands of cybersecurity incidents each day. The defenses the providers erect around their servers and their clients' data must importantly be up to date and redundant.

Despite the momentum in the market to rush to cloud-based P2P providers, I would caution governments to run full-fledged risk analyses to make sure that the data is secure, and that the provider is capable of protecting the systems and data against all possible threats. This is critical, because in the cloud, providers are housing millions of companies' data in one central location. If the servers, firewall or any connected system is compromised, it is entirely possible that thousands of companies and governments could have their financial data exposed to malicious actors.

Financial Risks for Public Financial Managers

While the primary focus of my analysis is the debate of cost savings and risk management between various on-prem and cloud-based P2P systems, this section will address the actual financial risks of poor cybersecurity. This is the most significant risk that should be weighed when making financial decisions related to software upgrades and maintenance.

First, however, we must discuss the differences between a cybersecurity incident and a cybersecurity breach, and the financial risks the two pose. Incidents are triggered when a malicious actor initiates a hack or assault on a secure data system with the intent to harm or create tangible damage. An incident is then categorized as a breach if actual damage or financial harm is created from the hack, through one of the three "CIA triad" areas: confidentiality, integrity and availability. If a malicious actor is deterred or stopped before damage materializes or information is stolen, it remains just a threat. However, if the

confidentiality of information, the integrity of the system itself or the availability of services to customers is impacted, it will be upgraded to a breach. The Council estimated the average cost of a breach in 2016 from the firms they sampled as $498 million per breach, with a total economic impact on the economy between $57 billion and $109 billion (The White House Council of Economic Advisors, 2018).

With such an outsize economic impact on the US economy, quality cybersecurity should be at the forefront for mitigating risks and often costly cyberattacks. From the Baltimore and Florida cases, it is clear that a simple ransomware attack could cost a significant sum of money, meaning public financial managers using legacy software should allocate appropriate resources to the protection of data, hardware and software used to process financial transactions. Importantly, we must recognize that cloud-based systems may take this budgetary impact off of the government itself, shifting it to the P2P provider, which is often more secure than what can be achieved through on-prem maintenance. Significant resources, particularly with on-prem legacy systems, should be dedicated to the mitigation of an incident becoming a breach.

FIGURE 3: Cyber Incidents and Breaches, 2016

	Incidents				Breaches			
Industry	Total	Small	Large	Unknown	Total	Small	Large	Unknown
Accomodation	215	131	17	67	201	128	12	61
Administrative	42	6	5	31	27	3	3	21
Agriculture	11	1	1	9	1	0	1	0
Construction	6	3	1	2	2	1	0	1
Education	455	37	41	377	73	15	15	43
Entertainment	5,534	7	3	5,524	11	5	3	3
Finance	998	58	97	843	471	39	30	402
Healthcare	458	92	108	258	296	57	68	171
Information	717	57	44	616	113	42	21	50
Management	8	2	3	3	3	2	1	0
Manufacturing	620	6	24	590	124	3	11	110

Mining	6	1	1	4	3	0	1	2
Other Services	69	22	5	42	50	14	5	31
Professional	3,016	51	21	2,944	109	37	8	64
Public	21,239	46	20,751	442	239	30	59	150
Real Estate	13	2	0	11	11	2	0	9
Retail	326	70	36	220	93	46	14	33
Trade	20	4	10	6	10	3	6	1
Transportation	63	5	11	47	14	3	4	7
Utilities	32	2	5	25	16	1	1	14
Unknown	8,220	3	1,089	7,128	68	2	15	51
TOTAL	**42,068**	**606**	**22,273**	**19,189**	**1,935**	**433**	**278**	**1,224**

There were 42,068 identified malicious cybersecurity incidents in 2016, of which 1,935 became breaches with tangible damages. To analyze the risk by sector, I created a "breach conversion rate" to identify which sectors were most likely to experience a conversion of an incident to a breach. Out of the total attacks, 4.6 percent of incidents converted to a breach. As indicated in Figure 2, the public sector was the target of over half of all incidents at 21,239, which is 2.6 times the incidents in "unknown", the second-highest target analyzed by the report. Because the highest-priority target for malicious actors is the government itself, management and financial administrators need to place a high budgetary priority on the security of government data. To this point, it appears the public sector is excelling. Out of 21,239 incidents, only 239 became breaches, for a conversion rate of 1.13 percent, the second lowest of any sector with over 500 incidents to Entertainment per Figure 3.

FIGURE 4: Breach Conversion Rate by Sector, 2016

Industry	Total	Small	Large	Unknown
Accomodation	93.49%	97.71%	70.59%	91.04%
Administrative	64.29%	50.00%	60.00%	67.74%
Agriculture	9.09%	0.00%	100.00%	0.00%
Construction	33.33%	33.33%	0.00%	50.00%
Education	16.04%	40.54%	36.59%	11.41%

Entertainment	0.20%	71.43%	100.00%	0.05%
Finance	47.19%	67.24%	30.93%	47.69%
Healthcare	64.63%	61.96%	62.96%	66.28%
Information	15.76%	73.68%	47.73%	8.12%
Management	37.50%	100.00%	33.33%	0.00%
Manufacturing	20.00%	50.00%	45.83%	18.64%
Mining	50.00%	0.00%	100.00%	50.00%
Other Services	72.46%	63.64%	100.00%	73.81%
Professional	3.61%	72.55%	38.10%	2.17%
Public	1.13%	65.22%	0.28%	33.94%
Real Estate	84.62%	100.00%	0.00%	81.82%
Retail	28.53%	65.71%	38.89%	15.00%
Trade	50.00%	75.00%	60.00%	16.67%
Transportation	22.22%	60.00%	36.36%	14.89%
Utilities	50.00%	50.00%	20.00%	56.00%
Unknown	0.83%	66.67%	1.38%	0.72%
ALL INCIDENTS	4.60%	71.45%	1.25%	6.38%

Alarmingly, the most vulnerable sector with over 500 incidents is Finance, as 47.9 percent of all incidents converted to a breach, but heavily skewed with smaller financial organizations converting 67.24 percent of the time. Large institutions fared better at 30.93 percent of instances converting. Also of note is the conversion rate of small public institutions when faced with an adverse cyber event at 65.22 percent. Smaller governments are more likely to run outdated systems due to cost and may not be able to fund proper IT departments, which increases the likelihood that an incident will convert. Management in small governments like those in the Florida cases should be vigilant about these threats and prepare room in the budget accordingly.

Most of the financial impact comes from sudden events. Cyberattacks are not random, but they are unpredictable without infrastructure to identify threats. The federal government has anti-espionage units and counter-cyberterrorism divisions within large departments like the

FBI, CIA and NSA that work to mitigate these risks (leading to the low .28 percent conversion rate of larger public institutions). Small governments have neither the budget nor the personnel availability to protect data like the federal government. The Florida towns saw a sizeable $400,000 and $600,000 cost to restore access to their computers, which may have on its own set a disturbing precedent that malicious actors may actually receive a financial payoff for ransomware attacks. Small governments will likely experience difficulty amassing the funds to make payments to hackers, resulting in budget cuts or added public debt. If a P2P system is breached and rendered useless, financial impacts could be exponentially higher as hackers could gain access to financial processes, or the government may need to replace the system altogether. Every function of government would be impacted from requisitions to reimbursements and even the budgeting process. Hardware may need to be replaced that has been rendered useless, compounding the financial impact on the government and its constituents. Proactive measures to prepare for an adverse cyber incident are critical cost saving measures, even if the government cannot afford to upgrade a system in its entirety.

RECCOMENDATIONS

It is difficult, if not impossible, to make a blanket recommendation about the upgrading of P2P software, as each institution has different goals – both budgetary and operationally – that impact software upgrade decisions. However, I have tailored my recommendations to both large and small governments respectively.

For large governments, I recommend the migration of P2P functions to the more secure and reliable cloud-based systems offered from providers. They are more flexible, up to date, and reduce maintenance costs by allowing reallocation or revision of the workforce that

maintains legacy systems. With larger budgets, more financial transactions and the increased threat that financial systems could be targeted, it is imperative that large governments avoid a repeat of the Baltimore EternalBlue hack by investing in financial software that safeguards the important financial information and financial processes. Any vulnerabilities in this software could be disastrous for budgets and continuity of services over time.

For smaller governments, my recommendation remains the same as larger governments, but often expensive software upgrades are not justifiable to constituents or those governing and developing budgets. Instead, I recommend a combination of outside cybersecurity consultants/managers and an increase in IT security staffing. While these are added costs, reducing the risk of an incident converting to a breach can be viewed as a cost-saving measure for governments.

CONCLUSION

In conclusion, this paper has explored and analyzed the financial savings P2Ps can provide, like workforce reductions, workflow eliminations, higher rates of on-contract purchases, tighter internal controls and software efficiency savings. I also analyzed the risks and ethical questions financial managers must evaluate when considering a software upgrade, particularly focusing on whether government can trust private companies with data, and whether cloud-based P2P softwares can provide better protection from cyberthreats. The answer was two-fold:

1. Cloud-based systems are often more secure than on-premise systems simply due to the redundancies and consistent security updates.
2. In some cases, government would be better off trusting financial data to private firms, particularly in smaller, understaffed governments.

P2P systems manage the entire financial process, even the budgeting and account processes at larger governmental institutions. Importantly, these systems are expensive to maintain, yet can provide significant cost savings over time. Efficiency gains and more modern user experience allow institutions to process more transactions with fewer staff, all while maintaining more control over spending. A legacy system may have provided the benefit of a single payment to own the software itself, yet they bring added costs in hardware, software developers and staff to maintain the integrity of the system. Other unrealized costs include those brought by often unintuitive systems that make purchasing contracts more obscure to end users. This can lead to increased spending off-contract, and when something goes wrong in the purchasing process with an off-contract vendor, staff may spend hours solving an issue, or goods may not be returned resulting in added costs.

Management should review the potential cost savings these modern, cloud-based softwares can provide and work to implement them if possible, particularly at smaller organizations that may have an unsecure system in place currently. While most governments have many varied priorities, P2P software can be justified to constituents as an initial investment for extended cost savings year-over-year. Current hardware and P2P software can speed up the government and provide higher-quality services to taxpayers.

Despite these benefits, there will always be risks associated with cloud-based P2P systems, particularly when it comes to cybersecurity. This paper explored the risks and costs poor cybersecurity can pose to institutions, and public financial managers should seek to allocate resources to protecting the government's systems and data. By investing in modern P2P software, governments can avoid serious expenses related to cyberthreats and breaches. As 5G

becomes more prevalent, P2P will certainly evolve beyond what it is today. Governments should prepare for the next evolution by modernizing their systems.

WORKS CITED

Biedron, R. (2018, August 21). The Procure-To-Pay Process Flow Explained. Retrieved June 09, 2019, from https://www.purchasecontrol.com/blog/procure-to-pay-cycle/

Center for Digital Government. (2018). Understanding Cloud Procurement: A Guide for Government Leaders. *Oracle Partner Network*.

Deloitte. (2018). Procure to Pay (P2P) Risk Analytics: Risk Advisory. *Deloitte*. Retrieved June 09, 2019, from https://www2.deloitte.com/content/dam/Deloitte/in/Documents/risk/in-risk-p2p-noexp.pdf

Farias, D. A., Romo, R. A., & Internation Business Machines Corp. (2000). *U.S. Patent No. US7711612B1*. Washington, DC: U.S. Patent and Trademark Office.

HFM. (2018, December 1). Taking a Holistic View of Procure to Pay. *Healthcare Financial Management*. Retrieved June 09, 2019, from http://web.b.ebscohost.com.ezproxy.uky.edu/ehost/pdfviewer/pdfviewer?vid=6&sid=9dda8422-cdbe-4ac9-bf3f-c1d336a753f0@pdc-v-sessmgr02

Miller, B. (2017, April 6). How Government Is Reforming IT Procurement and What it Means for Vendors. *Government Technology*. Retrieved June 09, 2019, from https://www.govtech.com/biz/How-Government-Is-Reforming-IT-Procurement-and-What-it-Means-for-Vendors.html

Pelroth, N., & Shane, S. (2019, May 25). In Baltimore and Beyond, a Stolen N.S.A. Tool Wreaks Havoc. *The New York Times*. Retrieved June 09, 2019, from https://www.nytimes.com/2019/05/25/us/nsa-hacking-tool-baltimore.html?searchResultPosition=8

Robinson, D. (2019, February 22). Search updated 2019 University of Kentucky employee salaries. Retrieved June 30, 2019, from https://www.kentucky.com/news/databases/article226745949.html

Sanderson, J., Lonsdale, C., & Mannion, R. (n.d.). *Towards a framework for enhancing procurement and supply chain management practice in the NHS: Lessons for managers and clinicians from a synthesis of the theoretical and empirical literature.* Southampton, United Kingdom: NIHR Journals Library.

SAP. (n.d.). Frequently Asked Questions. Retrieved June 10, 2019, from https://www.sap.com/about/trust-center/faq.html

SAP Ariba. (n.d.). Digitally Transform Your Business With SAP Ariba Solutions. Retrieved June 09, 2019, from https://www.ariba.com/solutions

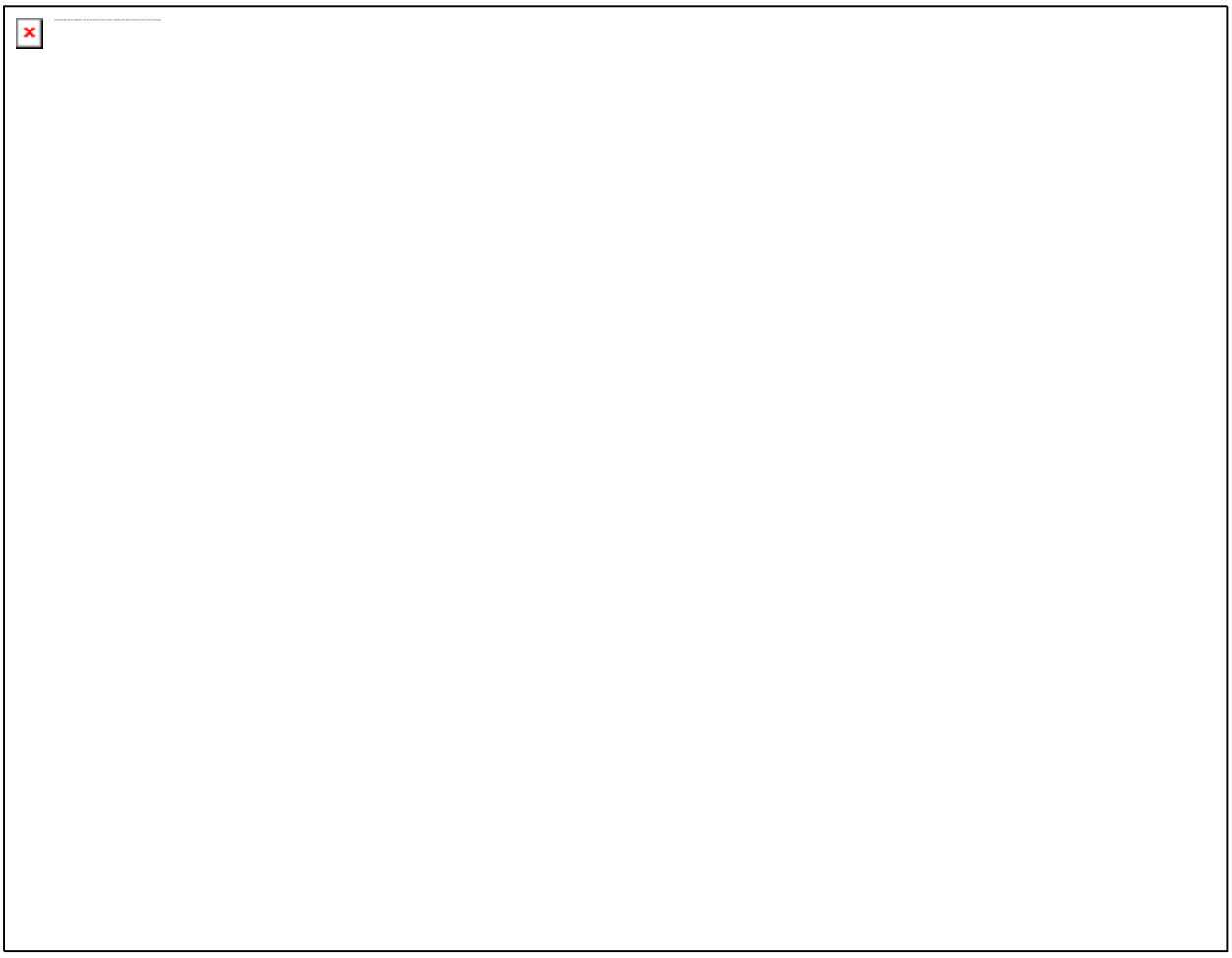
Walker, M. (2014, August 1). Purpose transforms public procurement. *Government Procurement*. Retrieved June 09, 2019, from http://web.a.ebscohost.com.ezproxy.uky.edu/ehost/pdfviewer/pdfviewer?vid=1&sid=4c6046cf-4b91-4413-9092-c72f3ed21fe3@sdc-v-sessmgr03

Warren, T. (2019, January 2). Windows 10 is now more popular than Windows 7. Retrieved June 27, 2019, from https://www.theverge.com/2019/1/2/18164916/microsoft-windows-10-market-share-passes-windows-7-statistics

White House Council of Economic Advisors, The. (2018, February). The Costs of Malicious Cyber Activity to the U.S. Economy. Retrieved June 5, 2019, from https://www.whitehouse.gov/wp-content/uploads/2018/03/The-Cost-of-Malicious-Cyber-Activity-to-the-U.S.-Economy.pdf

APPENDIX

APPENDIX 1: Data Security Incidents and Breaches with Conversion Rates, 2016



Source: The White House Council of Economic Advisors, 2018

APPENDIX 2: IRB Policies

Source: UKY Office of Research Integrity

Any activity that meets either (a) the Department of Health and Human Services (DHHS) definition of both "research" and "human subjects" or (b) the Food and Drug Administration (FDA) definitions of both "clinical investigation" and "human subjects" requires review and approval by the University of Kentucky (UK) IRB.

Research (DHHS): "a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge. Activities that meet this definition constitute research for purposes of this policy, whether or not they are conducted or supported under a program that is considered research for other purposes. For example, some demonstration and service programs may include research activities". [45 CFR 46.102(l)]

Human Subjects (**DHHS)**: "A living individual about whom an investigator (whether professional or student) conducting research: Obtains information or biospecimens through intervention or interaction with the individual, and uses, studies, or analyzes the information or biospecimens; or Obtains uses studies, analyzes, or generates identifiable private information or identifiable biospecimens." [45 CFR 46.102(e)]

- Intervention: includes both physical procedures by which information or biospecimens are gathered (e.g. venipuncture) and manipulations of the subject or the subject's environment that are performed for research purposes.
- Interaction: includes communication or interpersonal contact between investigator and subject.
- Identifiable: the identity of the subject is or may readily be ascertained by the investigator with the information obtained as part of the research.
- Private information: includes information about behavior that occurs in a context in which an individual can reasonably expect that no observation or recording is taking place, and information that has been provided for specific purposes by an individual and that the individual can reasonably expect will not be made public (*e.g.,* a medical record).
- Identifiable private information is private information for which the identity of the subject is or may readily be ascertained by the investigator or associated with the information.
- Identifiable biospecimen is a biospecimen for which the identity of the subject is or may readily be ascertained by the investigator or associated with the biospecimen.

  Clinical trial means a research study in which one or more human subjects are prospectively assigned to one or more interventions (which may include placebo or other control) to evaluate the effects of the interventions on biomedical or behavioral healthrelated outcomes. [45 CFR 46.102(b)]

  Clinical Investigation: "Involves use of a test article (i.e., drug, device, food substance or biologic), one or more human subjects, meets requirements for prior submission to FDA, or results are intended to be part of an application for research or marketing permit" [21 CFR 56.102]

Human Subjects (FDA): "An individual who is or becomes a participant in research, either as a recipient of the test article or as a control. A subject may be either a healthy individual or a patient." [21 CFR 56.102(e)] (Drug, Food, Biologic)

Human Subjects (FDA for medical devices): "A human who participates in an investigation, either as an individual on whom or on whose specimen an investigational device is used or as a control. A subject

may be in normal health or may have a medical condition or disease." [21 CFR 812.3(p)] (Medical Devices) NOTE: This definition includes use of tissue specimens even if they are unidentified.

In cases in which any other federal agency apply, institutional oversight of the activity follows the definitions for "research" and "human subjects" as defined by the relevant agency as appropriate. For Department of Defense-supported research, institutional oversight of the activity follows the definitions of "research" and "experimental subject" as defined by Department of Defense regulations [DoD Directive 3216.02].

The interviews in this capstone project are not subject to IRB review, as they did not obtain, use, study, analyze or generate identifiable private information or identifiable biospecimens per the guidelines above.

APPENDIX 3: Questions for Barry Swanson and James Frazier

1. What are the university's priorities when selecting a P2P system?

2. Why upgrade now?

3. Why a cloud-based system?
    A. Will this lead to savings over time?
    B. What risks did the university identify when exploring a cloud-based system?

4. Is the university more comfortable with an outside vendor protecting our data? Or is this just a necessary part of the system?

5. How is the university justifying/informing stakeholders of the expense of the program?

APPENDIX 4: Questions for Matt Perry

1. Are local servers more secure than cloud-based services? Why or why not?

2. Do you see the future of cloud-based storage as more secure than data stored at an institution itself?

3. Should governments weigh how comfortable they are with a private company holding their data before upgrading?
    A. What about small governments? They can't afford these upgrades—how do they stay safe?
    B. Are they more susceptible to breaches?

4. With a cloud-based system, would organizations still need to maintain their own cybersecurity teams?

5. How do cloud-based softwares provide security?